BUNDESREPUBLIK DEUTSCHLAND

CERTIFIED COPY OF
PRIORITY DOCUMENT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	199 57 387.5
Anmeldetag:	29. November 1999
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Aachen/DE
Bezeichnung:	Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung
IPC:	H 04 Q, H 04 L

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 8. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seiler

A 9161
06/00
EDV-L

PHD 99-174

ZUSAMMENFASSUNG

Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind. Erfindungsgemäß sendet das Funknetzwerk-Steuerung ein Schlüsseländerungsbefehl mit einem neuen Schlüssel an ein Terminal. Als Antwort sendet das Terminal einen Schlüsselbestätigungsbefehl mit dem empfangenen Schlüssel an die Funknetzwerk-Steuerung.

Fig. 4

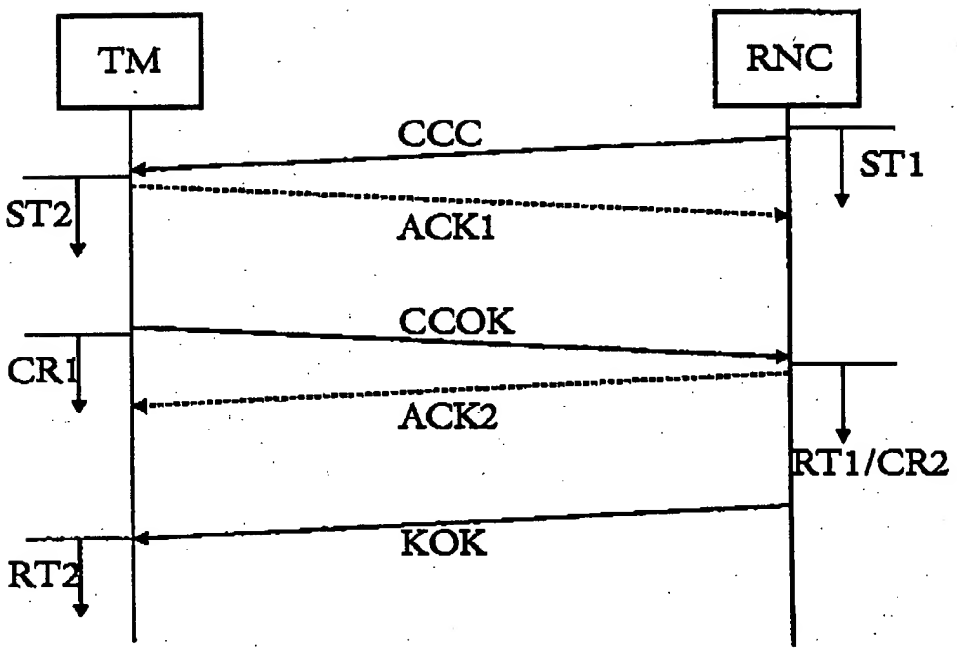

FIG. 4

BESCHREIBUNG

Drahtloses Netzwerk mit einer Prozedur zur Schlüsseländerung

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind.

Aus dem Buch „The GSM System for Mobile Communications" von Michel Mouly und Marie-Bernadette Pautet, Verlag Cell & Sys, 1992, Seiten 391 bis 395, ist bekannt, dass Daten zwischen einer Basisstation und einem Terminal verschlüsselt übertragen werden. Der für die Übertragung benötigte Schlüssel wird in bestimmten Zeitabständen verändert. Hierfür ist eine Prozedur in drei Schritten vorgesehen.

Der Erfindung liegt die Aufgabe zugrunde, ein drahtloses Netzwerk zu schaffen, das eine andere Prozedur zur Änderung eines Schlüssels angibt.

Die Aufgabe wird durch ein drahtloses Netzwerk der eingangs genannten Art dadurch gelöst,
dass die Funknetzwerk-Steuerung zur Sendung eines Schlüsseländerungsbefehl mit einem neuen Schlüssel an ein Terminal vorgesehen ist und
dass das Terminal zur Sendung eines Schlüsselbestätigungsbefehls mit dem empfangenen Schlüssel an die Funknetzwerk-Steuerung vorgesehen ist.

Unter dem erfindungsgemäßen drahtlosen Netzwerk ist ein Netzwerk mit mehreren Funkzellen zu verstehen, in denen jeweils eine Basisstation und mehrere Terminals Steuer- und Nutzdaten drahtlos übertragen. Eine drahtlose Übertragung dient zur Übertragung von Informationen z.B. über Funk-, Ultraschall- oder Infrarotwege.

Erfindungsgemäß bestätigt ein Terminal einen mit einem Schlüsseländerungsbefehl empfangenen neuen Schlüssel mit der Rücksendung des empfangenen Schlüssels an die

Funknetzwerk-Steuerung. Die Funknetzwerk-Steuerung empfängt diesen Schlüssel mit einem Schlüsselbestätigungsbefehl und vergleicht den gesendeten mit dem vom Terminal empfangenen Schlüssel. Erst wenn der Vergleich ergibt, dass der gesendete und der empfangene Schlüssel gleich ist, wird dieser neue Schlüssel von der Funknetzwerk-Steuerung verwendet. Das Terminal verwendet den neuen Schlüssel erst dann, wenn das Terminal einen Übereinstimmungsbefehl oder mit dem neuen Schlüssel verschlüsselte Daten von der Funknetzwerk-Steuerung empfängt. Durch diese Prozedur ist sichergestellt, dass Daten mit dem neuen Schlüssel von der Funknetzwerk-Steuerung verschlüsselt werden, wenn auch das Terminal diesen Schlüssel kennt.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Fig. näher erläutert. Es zeigen:

Fig. 1	ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren Terminals,
Fig. 2	ein Schichtenmodell zur Erläuterung verschiedener Funktionen eines Terminals oder einer Funknetzwerk-Steuerung,
Fig. 3	ein Blockschaltbild zur Erläuterung des Verschlüsselungsmechanismus in einem Terminal oder einer Funknetzwerk-Steuerung und
Fig. 4	einen Ablauf verschiedener Befehle bei einer Änderungsprozedur des für die Verschlüsselung benötigten Schlüssels.

In Fig. 1 ist ein drahtloses Netzwerk, z.B. Funknetzwerk, mit einer Funknetzwerk-Steuerung (Radio Network Controller = RNC) 1 und mehreren Terminals 2 bis 9 dargestellt. Die Funknetzwerk-Steuerung 1 ist für Steuerung aller am Funkverkehr beteiligten Komponenten verantwortlich, wie z.B. der Terminals 2 bis 9. Ein Steuer- und Nutzdatenaustausch findet zumindest zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 statt. Die Funknetzwerk-Steuerung 1 baut jeweils eine Verbindung zur Übertragung von Nutzdaten auf.

In der Regel sind die Terminals 2 bis 9 Mobilstationen und die Funknetzwerk-Steuerung 1 ist fest installiert. Eine Funknetzwerk-Steuerung 1 kann gegebenenfalls aber auch

beweglich bzw. mobil sein.

In dem drahtlosen Netzwerk werden beispielsweise Funksignale nach dem FDMA-, TDMA- oder CDMA-Verfahren (FDMA = frequency division multiplex access, TDMA = time division multiplex access, CDMA = code division multiplex access) oder nach einer Kombination der Verfahren übertragen.

Beim CDMA-Verfahren, das ein spezielles Code-Spreiz-Verfahren (code spreading) ist, wird eine von einem Anwender stammende Binärinformation (Datensignal) mit jeweils einer unterschiedlichen Codesequenz moduliert. Eine solche Codesequenz besteht aus einem pseudo-zufälligen Rechtecksignal (pseudo noise code), dessen Rate, auch Chiprate genannt, in der Regel wesentlich höher als die der Binärinformation ist. Die Dauer eines Rechteckimpulses des pseudo-zufälligen Rechtecksignals wird als Chipintervall T_C bezeichnet. $1/T_C$ ist die Chiprate. Die Multiplikation bzw. Modulation des Datensignals mit dem pseudo-zufälligen Rechtecksignal hat eine Spreizung des Spektrums um den Spreizungsfaktor $N_C = T/T_C$ zur Folge, wobei T die Dauer eines Rechteckimpulses des Datensignals ist.

Nutzdaten und Steuerdaten zwischen wenigstens einem Terminal (2 bis 9) und der Funknetzwerk-Steuerung 1 werden über von der Funknetzwerk-Steuerung 1 vorgegebene Kanäle übertragen. Ein Kanal ist durch einen Frequenzbereich, einen Zeitbereich und z.B. beim CDMA-Verfahren durch einen Spreizungscode bestimmt. Die Funkverbindung von der Funknetzwerk-Steuerung 1 zu den Terminals 2 bis 9 wird als Downlink und von den Terminals zur Basisstation als Uplink bezeichnet. Somit werden über Downlink-Kanäle Daten von der Basisstation zu den Terminals und über Uplink-Kanäle Daten von Terminals zur Basisstation gesendet.

Beispielsweise kann ein Downlink-Steuerkanal vorgesehen sein, der benutzt wird, um von der Funknetzwerk-Steuerung 1 Steuerdaten vor einem Verbindungsaufbau an alle Terminals 2 bis 9 zu verteilen. Ein solcher Kanal wird als Downlink-Verteil-Steuerkanal (broadcast control channel) bezeichnet. Zur Übertragung von Steuerdaten vor einem Verbindungsaufbau von einem Terminal 2 bis 9 zur Funknetzwerk-Steuerung 1 kann

beispielsweise ein von der Funknetzwerk-Steuerung 1 zugewiesener Uplink-Steuerkanal verwendet werden, auf den aber auch andere Terminals 2 bis 9 zugreifen können. Ein Uplink-Kanal, der von mehreren oder allen Terminals 2 bis 9 benutzt werden kann, wird als gemeinsamer Uplink-Kanal (common uplink channel) bezeichnet. Nach einem Verbindungsaufbau z.B. zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1 werden Nutzdaten über einen Downlink- und ein Uplink-Nutzkanal übertragen. Kanäle, die nur zwischen einem Sender und einem Empfänger aufgebaut werden, werden als dedizierte Kanäle bezeichnet. In der Regel ist ein Nutzkanal ein dedizierter Kanal, der von einem dedizierten Steuerkanal zur Übertragung von verbindungsspezifischen Steuerdaten begleitet werden kann.

Zur Einbindung eines Terminals 2 bis 9 zu einer Funknetzwerk-Steuerung 1 ist ein kollisionsbehafteter Kanal zuständig, der im folgenden als signalisierter RACH-Kanal (RACH = Random Access Channel) bezeichnet wird. Über einen solchen signalisierten RACH-Kanal können auch Datenpakete übertragen werden.

Damit Nutzdaten zwischen der Funknetzwerk-Steuerung 1 und einem Terminal ausgetauscht werden können, ist es erforderlich, dass ein Terminal 2 bis 9 mit der Funknetzwerk-Steuerung 1 synchronisiert wird. Beispielsweise ist aus dem GSM-System (GSM = Global System for Mobile communication) bekannt, in welchem eine Kombination aus FDMA- und TDMA-Verfahren benutzt wird, dass nach der Bestimmung eines geeigneten Frequenzbereichs anhand vorgegebener Parameter die zeitliche Position eines Rahmens bestimmt wird (Rahmensynchronisation), mit dessen Hilfe die zeitliche Abfolge zur Übertragung von Daten erfolgt. Ein solcher Rahmen ist immer für die Datensynchronisation von Terminals und Basisstation bei TDMA-, FDMA- und CDMA-Verfahren notwendig. Ein solcher Rahmen kann verschiedene Unter- oder Subrahmen enthalten oder mit mehreren anderen aufeinanderfolgenden Rahmen einen Superrahmen bilden. Aus Vereinfachungsgründen wird im folgenden von einem Rahmen ausgegangen, der als Referenzrahmen bezeichnet wird.

Die Steuer- und Nutzdatenaustausch über die Funkschnittstelle zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 kann mit dem in Fig. 2 dargestellten, bei-

spielhaften Schichtenmodell oder Protokollarchitektur (vgl. z.B. 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) RAN; Working Group 2 (WG2); Radio Interface Protocol Architecture; TS 25.301 V3.2.0 (1999-10)) erläutert werden. Das Schichtenmodell besteht aus drei Protokollschichten: der physikalischen Schicht PHY, der Datenverbindungsschicht mit den Unterschichten MAC und RLC (in Fig. 2 sind mehrere Ausprägungen der Unterschicht RLC dargestellt) und der Schicht RRC. Die Unterschicht MAC ist für die Medienzugriffssteuerung (Medium Access Control), die Unterschicht RLC für die Funkverbindungssteuerung (Radio Link Control) und die Schicht RRC für die Funkverwaltungssteuerung (Radio Resource Control) zuständig. Die Schicht RRC ist für die Signalisierung zwischen den Terminals 2 bis 9 und der Funknetzwerk-Steuerung 1 verantwortlich. Die Unterschicht RLC dient zur Steuerung einer Funkverbindung zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1. Die Schicht RRC steuert die Schichten MAC und PHY über Steuerungsverbindungen 10 und 11. Hiermit kann die Schicht RRC die Konfiguration der Schichten MAC und PHY steuern. Die physikalische Schicht PHY bietet der MAC-Schicht Transportverbindungen 12 an. Die MAC-Schicht stellt der RLC-Schicht logische Verbindungen 13 zur Verfügung. Die RLC-Schicht ist über Zugangspunkte 14 von Applikationen erreichbar.

Bei einem solchen drahtlosen Netzwerk werden die Daten aus Sicherheits- und Vertraulichkeitsgründen verschlüsselt über die Funkschnittstelle übertragen, um eine Abhören der Daten zu verhindern. Die Verschlüsselung wird in der Datenverbindungsschicht (z. B. in der RLC- oder MAC-Schicht) durchgeführt. Wie Fig. 3 zeigt, werden die Daten D über eine Exklusiv-Oder-Funktion (XOR) mit einer Verschlüsselungsmaske M verknüpft, so dass sich ein verschlüsselter Datenstrom C_D ergibt. Die Verschlüsselungsmaske M wird in einer Verschlüsselungs-Funktion 16 gebildet, die nach einem Verschlüsselungs-Algorithmus arbeitet und als Eingangswerte den Schlüssel CK und andere hier nicht näher dargestellte Parameter P erhält.

Der Schlüssel muss sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt sein. Dieser Schlüssel wird zu bestimmten Zeitpunkten geändert (z.B. alle 2 Stunden) mit einer speziellen Prozedur CKC (cipher key change), die als Schlüsseländerungs-Prozedur bezeichnet wird. Zuerst wird von der Funknetzwerk-Steuerung 1 (vgl.

Fig. 4) jede Übertragung von Daten zu dem Terminal (Downlink), welche verschlüsselt werden sollen, gestoppt (ST1). Die einzige Ausnahme ist ein im folgenden beschriebener Schlüsseländerungsbefehl CCC. Empfangene Uplink-Daten werden weiterhin mit dem bisherigen Schlüssel demaskiert. Dann wird von der Funknetzwerk-Steuerung 1 dem Terminal ein Schlüsseländerungsbefehl CCC mit einem neuen Schlüssel über einen Signalisierungskanal gesendet. Aus Sicherheitsgründen ist es unerheblich, ob Daten, die vor der Prozedur CKC mit dem alten Schlüssel verschlüsselt übertragen wurden, aber unquittiert (keine Bestätigung) blieben, nach der Prozedur CKC bei erneuter Übertragung nun mit dem neuen Schlüssel verschlüsselt werden.

Nachdem das Terminal den Schlüsseländerungsbefehl CCC mit dem neuen Schlüssel erhalten hat, wird nur ein Bestätigungsbefehl ACK1 zur Funknetzwerk-Steuerung 1 gesendet, damit die Funknetzwerk-Steuerung 1 nicht nach einer bestimmten Zeit den Schlüsseländerungsbefehl CCC mit dem neuen Schlüssel erneut sendet. Jede Übertragung von Daten (Uplink), welche verschlüsselt werden sollen, werden von dem Terminal ebenfalls gestoppt (ST2). Die einzige Ausnahme ist ein im folgenden beschriebener Schlüsselbestätigungsbefehl CCOK, der mit dem alten Schlüssel verschlüsselt wird. Nachdem das betreffende Terminal den Schlüssel aus dem Schlüsseländerungsbefehl CCC entnommen hat, wird der von dem Terminal aus dem Schlüsseländerungsbefehl CCC entnommene Schlüssel als neuer Schlüssel registriert und mit einem Schlüsselbestätigungsbefehl CCOK zur Funknetzwerk-Steuerung 1 gesendet. Das Terminal ist nach Sendung des Schlüsselbestätigungsbefehl CCOK bereit, Daten sowohl mit dem alten als auch mit dem neuen Schlüssel zu empfangen und zu entschlüsseln. Der alte Schlüssel wird nur dann benötigt, wenn ein erneuter Schlüsseländerungsbefehl CCC empfangen wird, der mit dem alten Schlüssel verschlüsselt worden ist. Dieses geschieht, wenn der in dem Schlüsselbestätigungsbefehl CCOK enthaltene Schlüssel von dem ursprünglich gesendeten z.B. infolge eines Übertragungsfehlers abweicht.

Der Empfang des Schlüsselbestätigungsbefehls CCOK wird von der Funknetzwerk-Steuerung 1 mit einem Bestätigungsbefehl ACK2 dem Terminal gemeldet und die Datenübertragung (Downlink) zum Terminal mit dem neuen Schlüssel wieder aufgenommen. Diese Wiederaufnahme erfolgt nur dann, wenn der ursprünglich gesendete

Schlüssel (ST1) mit dem in Schlüsselbestätigungsbefehl CCOK enthaltenen Schlüssel übereinstimmt (RT1). Empfangene Daten werden dann auch mit dem neuen Schlüssel demaskiert (CR2). Die Funknetzwerk-Steuerung 1 sendet dann einen Übereinstimmungsbefehl KOK zum Terminal. Wie oben erwähnt, muss die Sendung des Schlüsseländerungsbefehl CCC wiederholt werden, wenn die Schlüssel unterschiedlich sind. Nach Empfang dieses Übereinstimmungsbefehls KOK oder von Daten (Downlink), die mit dem neuen Schlüssel verschlüsselt worden sind, nimmt das Terminal die Datenübertragung (Uplink) mit dem neuen Schlüssel auf (RT2). Hiermit ist die Prozedur CKC abgeschlossen und somit wird die Datenübertragung nur mit diesem Schlüssel durchgeführt.

Dadurch, dass das Terminal zwischen CR1 und RT2 empfangene Daten sowohl mit dem alten als auch mit dem neuen Schlüssel entschlüsselt, kann das Terminal erkennen, ob die Prozedur CRC erfolgreich abgeschlossen wurde (dann empfängt das Terminal den Übereinstimmungsbefehl KOK verschlüsselt mit dem alten Schlüssel) oder ob die Prozedur erneut begonnen werden muss (dann empfängt das Terminal den Schlüsseländerungsbefehl CCC, der z.B. einen wiederum neuen Schlüssel enthält). Dadurch wird vermieden, dass infolge eines vom Terminal fehlerhaft empfangenen Schlüssels alle Verbindungen zwischen Terminal und Netzwerk abbrechen.

Die beschriebene Prozedur CKC bezieht sich zunächst nur auf die Signalisierungsverbindung. Datenverbindungen, die ebenfalls mit Übertragungswiederholungen arbeiten, werden in die Prozedur einbezogen, indem ihren jeweiligen Schichten RLC ebenfalls ein Stoppbefehl (Terminal: ST2, Netzwerk ST1) bzw. ein Befehl zur Wiederaufnahme der Übertragung von Nutzdaten mitgeteilt wird (Terminal: RT2, Netzwerk: RT1/CR2).

PATENTANSPRÜCHE

1. Drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten vorgesehen sind und die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten vorgesehen sind,
dadurch gekennzeichnet,
dass die Funknetzwerk-Steuerung zur Sendung eines Schlüsseländerungsbefehl mit einem neuen Schlüssel an ein Terminal vorgesehen ist und
dass das Terminal zur Sendung eines Schlüsselbestätigungsbefehls mit dem empfangenen Schlüssel an die Funknetzwerk-Steuerung vorgesehen ist.

2. Drahtloses Netzwerk nach Anspruch 1,
dadurch gekennzeichnet,
dass die Funknetzwerk-Steuerung zur Sendung eines Übereinstimmungsbefehls an das Terminal vorgesehen ist, wenn der empfangene Schlüssel mit dem gesendeten Schlüssel übereinstimmt.

3. Drahtloses Netzwerk nach Anspruch 2,
dadurch gekennzeichnet,
dass das Terminal zur Verwendung des von der Funknetzwerk-Steuerung empfangenen Schlüssels bei der Verschlüsselung von Daten vorgesehen ist, wenn das Terminal den Übereinstimmungsbefehl oder mit dem neuen Schlüssel verschlüsselte Daten empfängt.

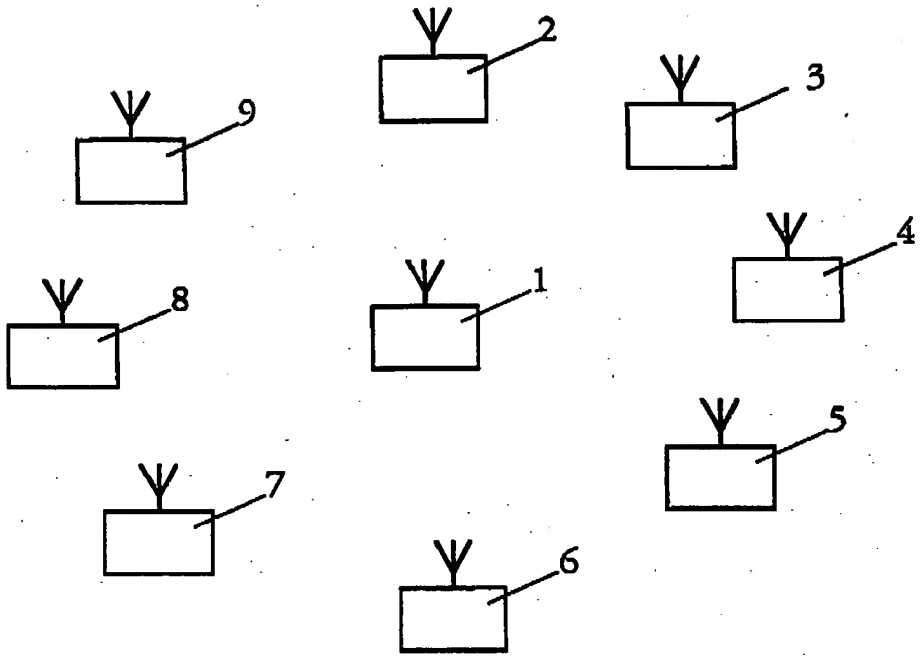

FIG. 1

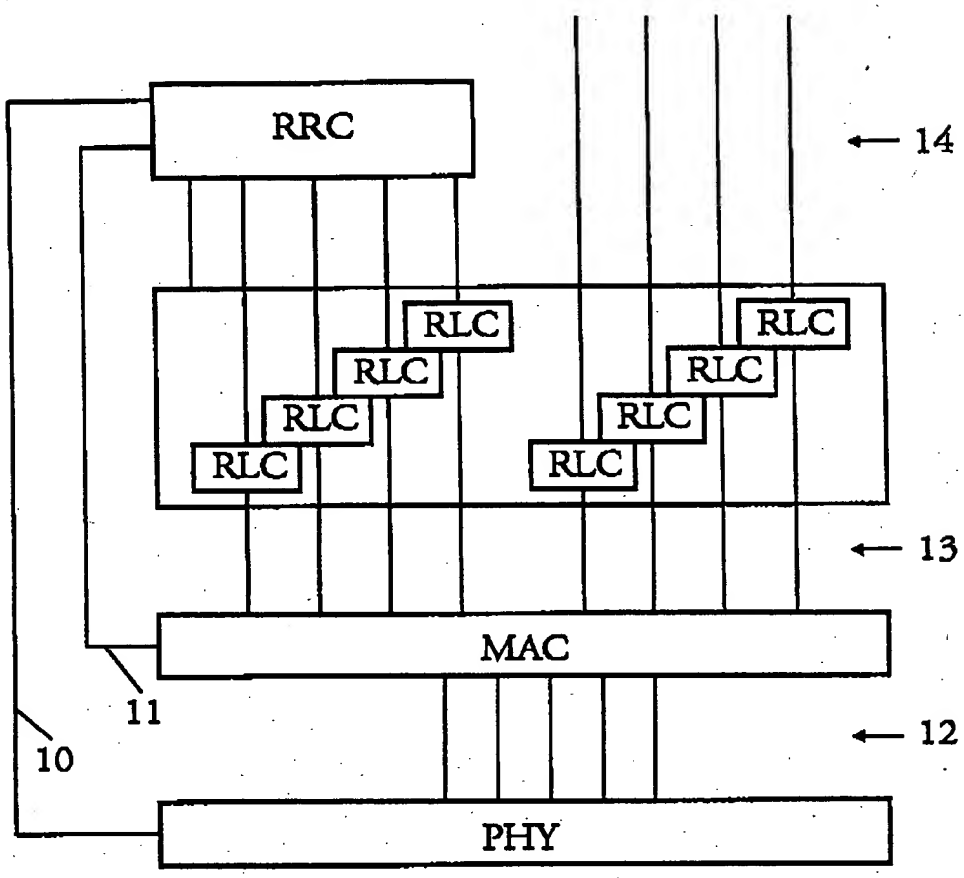

FIG. 2

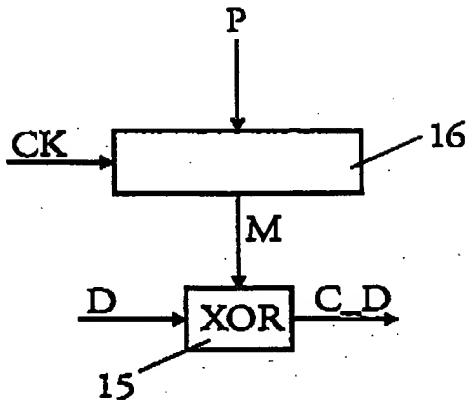

FIG. 3

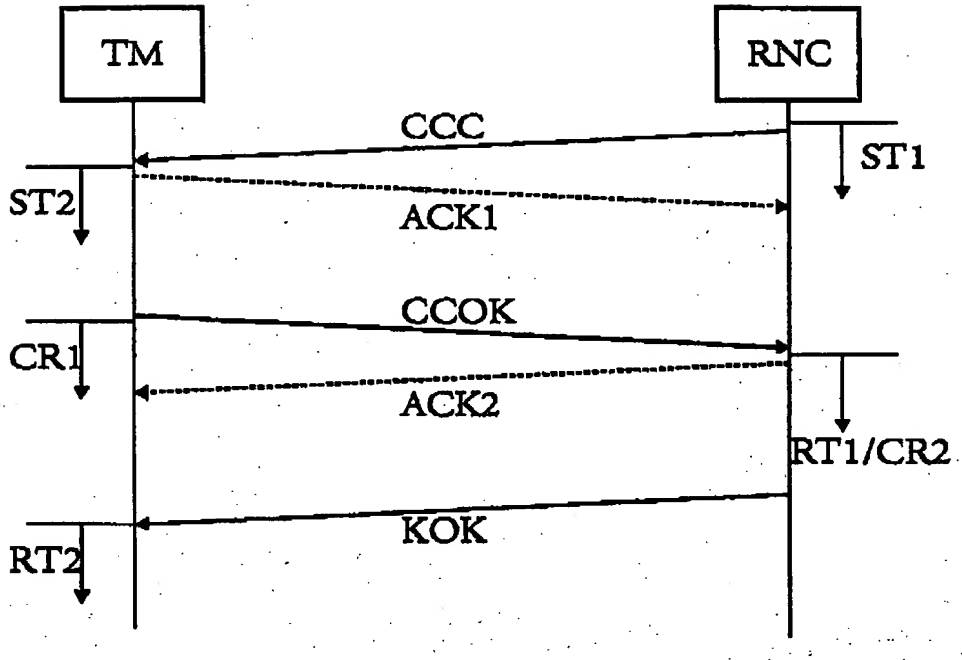

FIG. 4